Flight Software Design Choices Based on Criticality

Earl Lee

281-282-4331

earl.l.lee@usahq.unitedspacealliance.com

United Space Alliance

Introduction

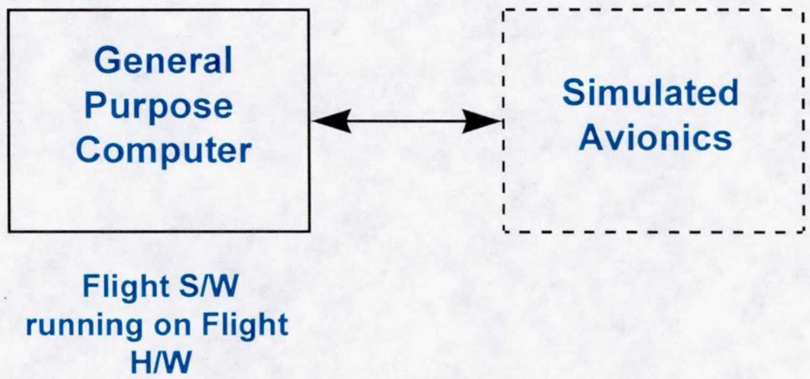
- Realities of Man Rated systems
- Realities of centralized processing
- Criticality independent improvements
- Criticality dependent improvements
- Criticality dependent architecture decisions
- Partitioning by criticality
- Mission critical development option

High Criticality: Necessary Caution

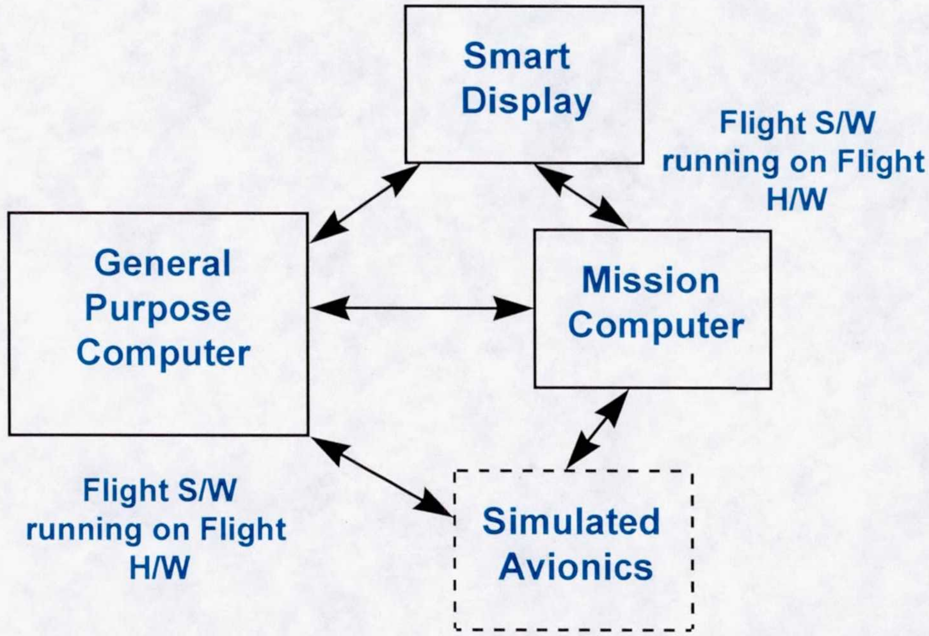
- What high criticality means for Space Shuttle
  - Human life is dependent on correct operation
    - Drives emphasis on quality, reliability, safety
      - Controlled, predictable, and repeatable development processes
      - Analysis of all software errors for flight safety impact
      - Methods open to defect cause analysis
      - Development and test tools also treated as critical
  - Flight Support requires near immediate response
    - Corrections or work arounds expected during operational use
    - Delivery in hours
    - Developed following a stringent process

Software Test Environment Complexity

Centralized Processing



Distributed Critical Processing



Less Critical: Caution & Culture

- Flexibility should be permitted when the consequences of software failure are non-life threatening
  - Expected software quality is consequence driven
    - Less costly development methods
    - Less costly defect control process
    - Less oversight of development processes
  - Flight Support levels are consequence driven
    - Less extraordinary support requirements
    - Recovery more important than immediate understanding of cause
    - Corrections by release, not by patch
- Flight Critical culture may require actions which are inconsistent with failure consequences
  - Decades of centralized processing have institutionalized high criticality thinking

Choosing COTS Software Trade Candidates

Trade for High Criticality Usage	Trade for Lower Criticality Usage
Software Production Process	Flight Support
Flight Support	Technical Suitability
Technical Suitability	System Compatibility
System Compatibility	Product Longevity Assessment
Product Longevity Assessment	Technical Support
Technical Support	Cost
Cost	

- Equivalent criteria
- Unique criteria
- Scalable criteria

COTS Decision Guidance

Selecting COTS/MOTS for high criticality functions should require greater technical insight and stronger risk management planning than for lower criticality functions

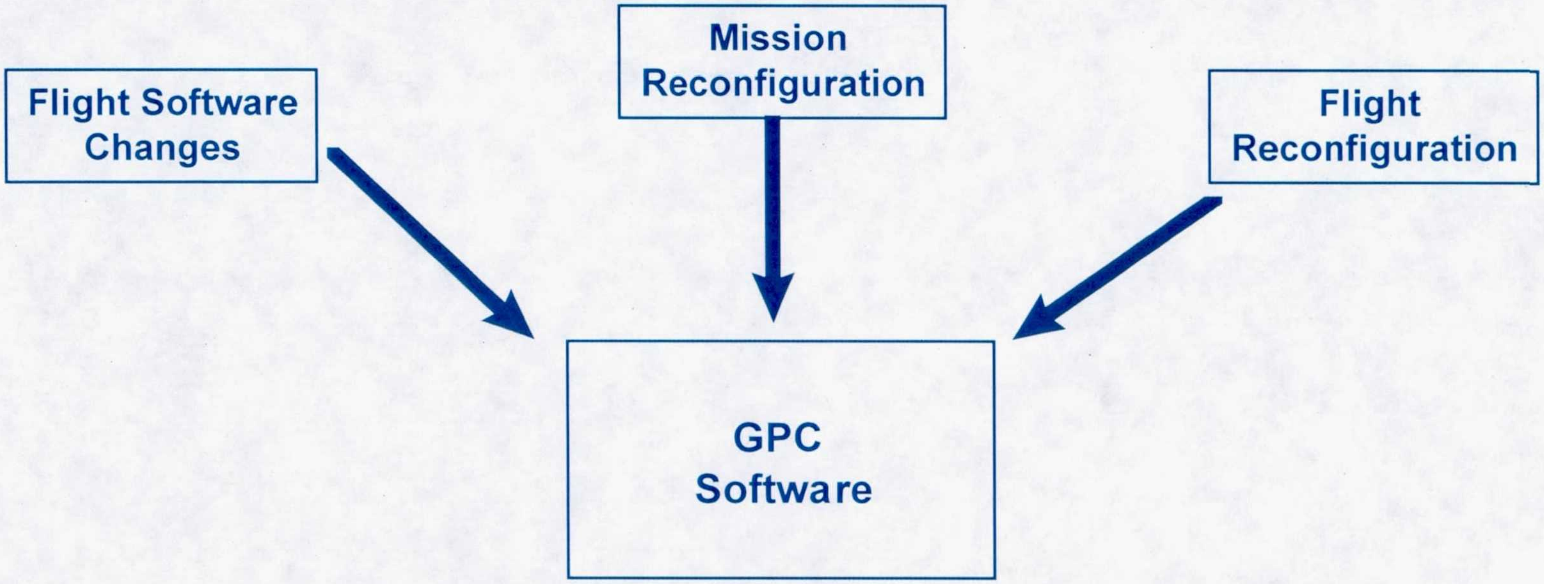
High Criticality

Is Certification Plan adequate for criticality?
Will vendor disclose defects found by other users?
Are there adequate measures of quality and reliability?
Will vendor disclose development methods?
Is vendor willing to escrow source code?
Visibility into design and code?
Is Flight Support Plan adequate?
Is technical support plan adequate?
Is the risk management plan for loss of support adequate?

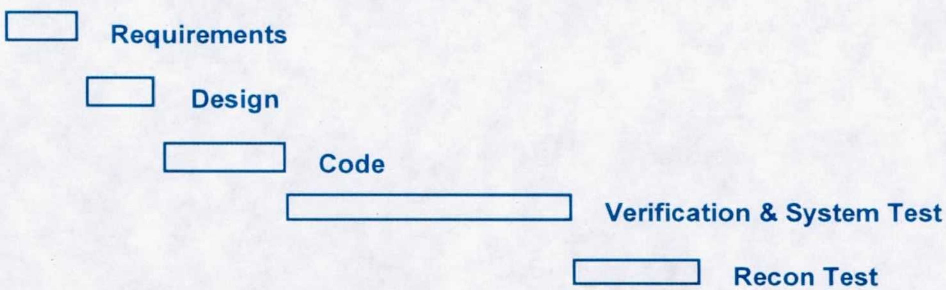
Lower Criticality

Is Certification Plan adequate for criticality?
Will vendor disclose defects found by other users?
Is vendor willing to escrow source code?
Is Flight Support Plan adequate?
Is technical support plan adequate?
Is the risk management plan for loss of support adequate?

Realities of Centralized Processing



Flight Critical Development Processes



Criticality Independent Improvements

- Technology modernization enables process improvements independent of software criticality
  - Requirements Definition and Analysis Phase
    - On-line requirements and on-line reviews
    - Requirements prototyping
  - Software Development and Verification Phase
    - Visual presentation of design
    - Design directly coupled to code
    - Modern desk-top development tools
    - Automatic path/segment test tools including coverage analysis
    - LAN based simulations
    - Automatic test report generation

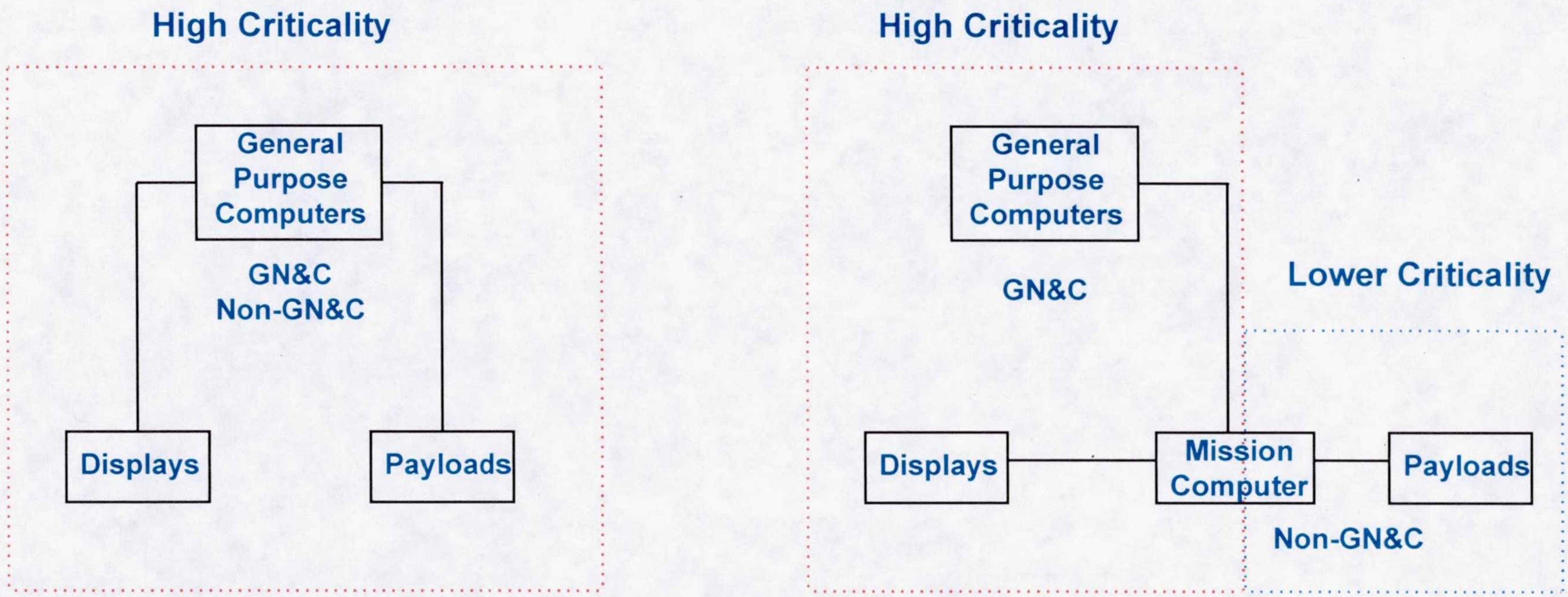
- Potential development cost reduction of ~10% for new avionics software compared to current methods

Criticality Dependent Changes

- Candidate process changes based on a criticality partitioned system
  - V&V testing to vary with criticality of functionality
  - Redundant testing coverage (like today) for Criticality 1 software
  - Less than full shall & path coverage for lower criticality software
    - Reduced testing documentation
    - Random sampling of V&V test results for NASA review
  - Test philosophies to be evaluated with various combinations of V&V testing and analysis or audit

- Potential development cost reduction of ~22% for new avionics software compared to current methods

Criticality Isolation Is Difficult to Achieve

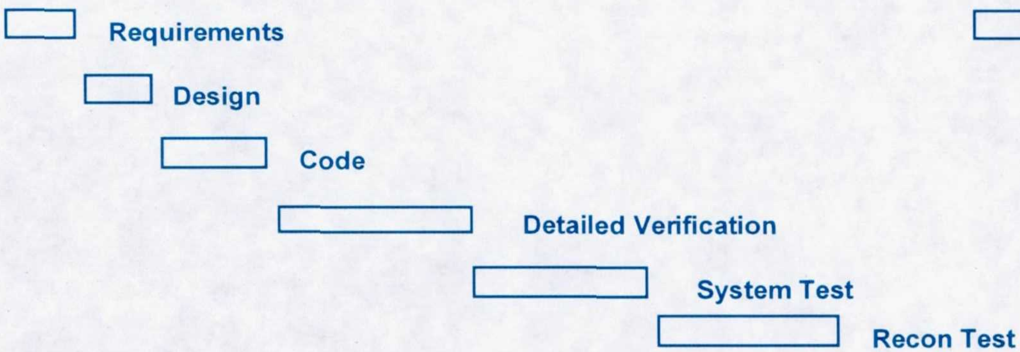


Partitioning by Criticality

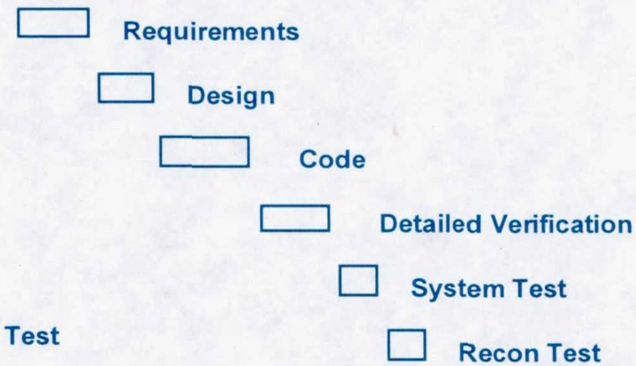
Flight Critical GPC's

Mission Critical Processor

Flight Critical Development Process



Mission Critical Development Process



Selecting a Process to Match Criticality

- Sample predicted defects remaining at first flight (per 100K SLOCS)
- SAMPLE DATA - Not final quantitative values

Errors Remaining			
Inserted Errors/KSLOC	10		1,000 Errors
Removed in Inspection	65% of Total		350 Errors
Development Test	55% of Remaining		150 Errors
Software Integration Test	50% of Remaining		75 Errors
After V&V Testing			
Criticality 1 Test Philosophy		80% of Remaining	15 Errors
Criticality 2 Test Philosophy		60% of Remaining	30 Errors
Criticality 3 Test Philosophy		40% of Remaining	45 Errors
After Integrated Avionics Verification Testing			
Criticality 1 Test Philosophy		65% of Remaining	5 Errors

Life Cycle Support

GPC S/W		New Avionics S/W	
System Software	$	COTS RTOS	$
Flight Critical	$	+ Non-Flight Critical	$
- Non Flight Critical	$	S/W Dev. Facility	$
S/W Prod. Facility	$		$$
	$$$		

Partitioning for criticality limits support costs for new avionics

Summary

- Man Rated systems require added caution
- Distributed processing increases the software verification boundaries
- Select COTS with care and take appropriate risk mitigation actions
- Single criticality forces a single process
- Partitioning enables flexibility in process selection
- Appropriate process tailoring necessary to yield required costs and quality
- Criticality partitioning is key to controlling costs